ОДЛУКА
О УПРАВЉАЊУ ИНФОРМАЦИОНИМ СИСТЕМОМ И
РИЗИЦИМА ИНФОРМАЦИОНЕ И КОМУНИКАЦИОНЕ ТЕХНОЛОГИЈЕ
У БАНЦИ
(„Службени гласник Републике Српске“, број 42/25)

Подручје	**Одговорности**
Датум одговора	10.02.2026.
Тема	**Управљање информационом безбједношћу** (члан 4. став 1. тачка 3)
	(1) Надзорни одбор банке дужан је, као минимум, да: *…3) обезбиједи да управљање информационом безбједношћу у свом раду и линији извјештавања буде независно од управљања ИКТ системом*
Питање банке бр. 1	Појашњење предметне одредбе да управљање информационом безбједношћу у свом раду и линији извјештавања треба да буде независно од управљања ИКТ системом.
Одговор Агенције	Управљање информационом безбједношћу, као један од ризика ИКТ система, саставни је дио управљања ризицима ИКТ система банке. Организациона јединица задужена за управљање ИКТ системом организационо је и функционално одвојена од организационе јединице надлежне за управљање информационом безбједношћу и има независне линије извјештавања према Управи банке. Организациона јединица задужена за управљање ИКТ системом одговара члану Управе надлежном за управљање ИКТ системом, док функција управљања информационом безбједношћу, без обзира на њену организациону позицију, одговара члану Управе надлежном за управљање ризицима. Члан Управе надлежан за управљање ИКТ системом не може истовремено бити одговоран за управљање ИКТ ризицима, укључујући и ризике информационе безбједности.
Подручје	**Одговорности**
Датум одговора	10.02.2026.
Тема	**Праћење уговора о употреби ИКТ услуга** (члан 5. став 1. тачка 10.)
	(1) Управа банке је дужна, као минимум, да: *…10) успостави функцију за праћење уговора о употреби ИКТ услуга склопљених са трећим странама или именује члана вишег руководства који ће бити одговоран за надзор над повезаним ризицима и релевантном документацијом,*
Питање банке бр. 2	Функција за праћење уговора - да ли се односи на праћење екстернализованих уговора или свих уговора који се доводе у везу са ИКТ системом? Потребно је прецизирати која се релевантна документација подразумјева и ризици - или се примјењује одредбе Одлуке о управљању екстернализацијом на овај дио?
	Наведеном одредбом прописује се обавеза Управе банке да обезбиједи адекватан надзор над ризицима који произилазе из коришћења ИКТ услуга трећих страна (нпр. outsourcing, cloud услуге,

	одржавање система и сл.), као и над релевантном документацијом. Захтјев се може испунити на један од два начина: 1. успостављањем посебне функције у оквиру организационе структуре банке, чији је задатак континуирано праћење уговора о употреби ИКТ услуга склопљених са трећим странама, укључујући идентификацију, процјену и праћење повезаних ИКТ и оперативних ризика, или 2. именовањем члана вишег руководства који ће бити јасно и формално одговоран за надзор над наведеним уговорима, повезаним ризицима и релевантном документацијом. Банка постојеће добре праксе из домена управљања екстернализацијом може проширити и на управљање ризицима који су везани за остале пружаоце ИКТ услуга. Уколико банка има успостављен Одбор за управљање екстернализацијом, наведена функција надзора над уговорима о употреби ИКТ услуга може бити укључена у надлежности тог Одбора.
Подручје	**Одговорности**
Датум одговора	10.02.2026.
Тема	**Тијело за координацију активности које се односе на ИКТ систем** (члан 5. став 5.)
	(5) Управа банке је дужна размотрити потребу формирања посебног тијела које ће координисати активности које се односе на ИКТ систем, узимајући у обзир величину банке, природу, обим и сложености својих услуга, активности и пословања, унутрашњу организацију, те величину и комплексност ИКТ система.
Питање банке бр. 3	Да ли се као посебно формирано тијело може сматрати већ постојећи Одбор за управљање информационим системом банке?
Одговор Агенције	Уколико Управа Банке закључи да банка има потребу за формирањем посебног тијела, то може бити постојећи Одбор за управљање информационим системом банке.
Подручје	**Одговорности**
Датум одговора	10.02.2026.
Тема	**Лице одговорно за информациону безбједност** (члан 6. став 1.)
	(1) Лице одговорно за информациону безбједност треба бити компетентно лице с одговарајућим стручним квалификацијама, специјалистичким знањима и искуством у области управљања информационом безбједношћу и при том посједује релевантне међународно признате сертификате из ове области.
Питање банке бр. 4	Шта се сматра релевантним међународно признатом сертификатом из ове области?
Одговор Агенције	Релевантним међународно признатим сертификатима сматрају се сертификати из области информационе безбједности који су признати у банкарској и финансијској индустрији, при чему се ISO/IEC 27001 (Lead Implementer или Lead Auditor) сматра минималним стандардом, а сертификати попут CISSP и CISM додатним показатељем напредних стручних и управљачких компетенција, као и други међународно признати сертификати из области управљања информационом

	безбједношћу и ИКТ ризицима (нпр. CISA, CRISC, ISO/IEC 27005), у зависности од сложености информационог система и ризичног профила банке.
Подручје	**Одговорности**
Датум одговора	10.02.2026.
Тема	**Лице одговорно за безбједност ИС** (члан 6. став 2.)
	(2) Лице из става 1. овог члана треба да надзире и координише активности у вези са информационом безбједношћу, а што укључује најмање сљедеће: *1) координише и спроводи интерне контроле у складу са овом одлуком и релевантним стандардима,*
Питање банке бр. 5	Да ли значи да лице одговорно за безбједност информационог система, у складу са одредбама наведеног члана, постаје контролна функција у банци?
Одговор Агенције	Банка је у складу са чланом 5. став 4. дужна да осигура потребне и адекватне ресурсе за управљање ИКТ ризицима на континуираној основи, што значи да банка у контролној функцији управљања ризицима мора имати запослене са одговарајућим стручним квалификацијама и вјештинама за управљања ИКТ ризицима, што укључује и процјену ИКТ ризика. С обзиром на овај захтјев банка може функцију управљања безбједношћу информационог система успоставити унутар контролне функције управљања ризицима.
Подручје	**Одговорности**
Датум одговора	10.02.2026.
Тема	**Лице одговорно за информациону безбједност** (члан 6. став 2. тачка 3)
	(2) Лице из става 1. овог члана треба да надзире и координише активности у вези са информационом безбједношћу, а што укључује најмање сљедеће: *…3) учествује у активностима идентификације и процјене ИКТ ризика и пружању приједлога мјера за управљање ИКТ ризицима из чланова 15. – 19. ове одлуке*
Питање банке бр. 6	Да ли лице одговорно за информациону безбједност треба само да учествује или може и да буде лице одговорно за управљање ИКТ ризицима?
Одговор Агенције	У складу са Одлуком, банка је дужна да одреди лице одговорно за безбједност информационог система, које учествује у активностима идентификације и процјене ИКТ ризика, као и у предлагању мјера за управљање ИКТ ризицима. У складу са начелом пропорционалности, банка може организовати ову функцију као засебну функцију, или у оквиру функције управљања ИКТ ризицима, под условом да су обезбијеђени адекватни кадровски капацитети, јасно дефинисане надлежности и независност у обављању послова.
Подручје	**Одговорности**
Датум одговора	10.02.2026.
Тема	**Спољна ревизија информационог система** (члан 8.)

	(1) Банка је у обавези да спроводи спољну ревизију ИКТ система на годишњем нивоу, у складу са Законом и подзаконским актима Агенције који регулишу област спољне ревизије у банкама, уколико одредбама ове одлуке није другачије дефинисано.
Питање банке бр. 7	У члану 8. Одлуке није прописано ко усваја извјештај екстерног ревизора информационог система.
Одговор Агенције	Извјештај о ревизији информационог система, сачињен од стране спољног ревизора, усваја Надзорни одбор банке.
Подручје	**Спољна ревизија**
Датум одговора	10.02.2026.
Тема	**Извјештај о обављеној ревизији ИКТ система** (члан 8. став 7)
	(7) Извјештај о обављеној ревизији ИКТ система је посебан извјештај, који је банка дужна доставити Агенцији најкасније до 30. априла текуће године.
Питање банке бр. 8	Да ли ће се ова обавеза примијењивати од 1.1.2026. године?
Одговор Агенције	Банка је дужна своје пословање ускладити са одредбама Одлуке до 1.4.2026, што се односи и на ову одредбу.
Подручје	**Управљање ИКТ системом**
Датум одговора	10.02.2026.
Тема	**Стратегија ИКТ система** (члан 9. став 2. тачка 3.)
	(2) Стратегија ИКТ система из става 1. тачка 1) овог члана, треба да: *…3) дефинише јасне циљеве у погледу информационе безбједности, укључујући кључне показатеље успјешности и кључне параметре ризика.*
Питање банке бр. 9	Шта се подразумијева под кључним показатељима успјешности/ кључним параметрима ризика, односно да ли исто треба да буде уврштено и у оквире цјелокупне толеранције банке на ризике?
Одговор Агенције	Стратегијом ИКТ система утврђују се кључни показатељи успјешности (KPI) и кључни параметри ризика (KRI), који омогућавају праћење: - степена усклађености ИКТ система са пословним циљевима банке, - стабилности и доступности ИКТ система, - нивоа информационе безбједности, - управљања ИКТ ризицима, укључујући неприхватљиве ризике, и - развоја ИКТ капацитета. KPI/KRI се наводе квантитативно и/или квалитативно, на примјер: - проценат доступности критичних ИКТ система: ≥ 99%, - број значајних ИКТ инцидената који утичу на критичне функције: ≤ 2 годишње, - проценат критичних и високих рањивости које су елиминисане или ублажене у року – циљ: 100%, - ојачавање (*hardening*) система: X% система усклађено у односу на препоручене сигурносне конфигурације. Циљ: повећање за Y% квартално,

	- степен успјеха на симулацији фишинга: X% запослених који нису кликнули на симулирани фишинг мејл у кварталној кампањи. Циљ: повећање. За сваки KPI/KRI стратегија треба да дефинише: како се мјери (метрика), ко је одговоран и периодичност извјештавања. Детаљни показатељи, циљне вриједности и начин праћења дефинишу се кроз оперативне планове и прате се путем редовних извјештаја Управи банке у складу са чланом 10.
Подручје	**Управљање ИКТ системом**
Датум одговора	10.02.2026.
Тема	**ИКТ системи, протоколи и алати (**члан 11. став 2. тачка 4.)
	(2) Банка је дужна да користи и одржава ажурним ИКТ системе, протоколе и алате који су: *...4) технолошки отпорни како би се на адекватан начин носили са додатним потребама за обрадом података у условима стресног тржишта или других неповољних ситуација.*
Питање банке бр. 10	На који начин ће Банка вршити процјену технолошке отпорности која је прописана чланом 11. став 2. тачка 4. Одлуке?
Одговор Агенције	Банка треба да користи и одржава ажурним ИКТ системе, протоколе и алате, који су технолошки отпорни, а имајући у виду најбоље безбједносне препоруке и праксе. Процјену своје технолошке отпорности проводи кроз идентификацију и класификацију пословних функција, мапирање информационе и ИКТ имовине и њихових међузависности, процјену ИКТ ризика и адекватности успостављених мјера заштите, укључујући провођење редовних тестирања безбједности ИКТ система (нпр. пенетрациона тестирања и процјене рањивости), тестирање планова континуитета пословања у подручју ИКТ-а, планова одговора и опоравка ИКТ система, укључујући и тестирање опоравка резервних копија података, као и праћење и анализу ИКТ инцидената. Процјена технолошке отпорности обухвата и свеобухватну оцјену способности банке да одржи стабилно функционисање ИКТ система и да се носи са повећаним потребама за обрадом података у условима стресног тржишта, ванредних околности и других значајних поремећаја.
Подручје	**Управљање ИКТ ризицима**
Датум одговора	10.02.2026.
Тема	**Оквир за управљање ИКТ ризицима** (члан 14. став 1.)
	(1) Оквир за управљање ИКТ ризицима, треба да обухвати најмање: стратегије, политике, методологије, програме, процедуре и планове, те ИКТ протоколе и алате који су неопходни за адекватну заштиту информационе имовине и ИКТ имовине, како би се утицај ИКТ ризика свео на најмању могућу мјеру.
Питање банке бр. 11	Да ли се под оквиром за управљање ИКТ ризицима подразумијевају све стратегије, политике, методологије и др. акти које банка доноси из домена ИКТ-а и безбједности информационог система а чијом се примјеном утиче на смањење ИКТ ризика?

Одговор Агенције	Оквир за управљање ИКТ ризицима обухвата све стратегије, политике, методологије и друге интерне акте које банка доноси у области ИКТ-а и безбједности информационог система, а чијом се примјеном утиче на смањење ИКТ ризика, као и све друге елементе који омогућавају банци да системски идентификује, мјери, контролише и прати ИКТ ризике, са циљем да се њихов утицај сведе на најмању могућу мјеру, укључујући ИКТ протоколе и алате (нпр. шифровање, VPN, механизме аутентификације, SIEM системе, алате за управљање рањивостима и закрпама, системе за резервне копије и опоравак података и др.).
Подручје	**Управљање ИКТ ризицима**
Датум одговора	10.02.2026.
Тема	**Пословне функције** (члан 15. став 1)
	(1) У оквиру система за управљање ИКТ ризицима банка је дужна идентификовати, класификовати и адекватно документовати све пословне функције које подржава ИКТ, улоге и одговорности, информациону имовину и ИКТ имовину која подржава те функције, као и њихове улоге и зависности у односу на ИКТ ризик. Банка је дужна према потреби, а најмање на годишњем нивоу, преиспитати примјереност класификације и релевантне документације.
Питање банке бр. 12	Шта се подразумијева под класификацијом пословних функција? Да ли се подразумијева израда регистра/евиденције класификације и релевантне документације која ће се преиспитивати минимум једном годишње?
Одговор Агенције	У складу са ставом 2. приликом провођења класификације пословних функција банка је дужна размотрити захтјеве у погледу повјерљивости, интегритета и доступности, те процијенити укупан ниво ИКТ ризика за сваку пословну функцију. У складу са ставом 6. банка је дужна да успостави адекватну евиденцију и да је редовно ажурира, а обавезно након значајних промјена. Резултат класификације може бити регистар пословних функција или евиденција у неком другом облику, која обавезно садржи резултате класификације у односу на повјерљивост, интегритет и доступност, као и утврђени ниво ИКТ ризика за сваку пословну функцију.
Подручје	**Управљање ИКТ ризицима**
Датум одговора	10.02.2026.
Тема	**Информациона имовина** (члан 15. став 3)
	(3) Банка је дужна идентификовати сву информациону имовину и ИКТ имовину, укључујући и ону на удаљеним локацијама, мрежне ресурсе и хардверску опрему те мапирати критичну и кључну информациону и ИКТ имовину и јасно одредити одговорност за имовину. Такође, неопходно је мапирати конфигурацију информационе и ИКТ имовине, као и везе и међузависности између различитих информационих и ИКТ ресурса.
Питање банке бр. 13	Шта се подразумијева под конфигурацијом информационе и ИКТ имовине?

	Ко је одговоран за класификацију информационе имовине?
Одговор Агенције	Под „конфигурацијом информационе и ИКТ имовине“ подразумијева се актуелна конфигурација свих софтверских и хардверских компоненти информационог система банке (нпр. за сервер: серијски број, модел, локација, верзија оперативног система, апликације које се хостују, администратор). Банка је дужна мапирати све компоненте, њихове међузависности, критичне и кључне елементе, као и одговорности за њихово управљање. Власник информационе имовине је одговоран за њену класификацију.
Подручје	**Управљање ИКТ ризицима**
Датум одговора	10.02.2026.
Тема	**Изложеност ИКТ ризицима од других финансијских субјеката** (члан 15. став 5.)
	(5) Банка је дужна континуирано идентификовати све изворе ИКТ ризика, посебно изложеност ризицима од других финансијских субјеката и према њима, те процјењивати сајбер пријетње и рањивости ИКТ-а које су релевантне за њихове пословне функције подржане ИКТ-ом, информациону и ИКТ имовину. Банка је дужна редовно, а најмање једном годишње, преиспитати сценарије ризика који утичу на њих.
Питање банке бр. 14	На које финансијске субјекте, као изворе изложености ИКТ ризицима, се мисли, а који су прописани наведеним чланом? Такође, на који начин ће Банка процјењивати пријетње и рањивости ИКТ-а које су релевантне за њихове пословне функције подржане ИКТ-ом, информациону и ИКТ имовину?
Одговор Агенције	Банка спроводи континуирану идентификацију ИКТ ризика кроз: - успостављање и редовно ажурирање регистра информационе и ИКТ имовине, редовне годишње процјене ризика, као и процјене ризика при увођењу нових система или услуга, након значајних промјена или насталих инцидената, - процјену изложености ризицима који произилазе из сарадње са другим финансијским субјектима (кореспондентске банке, инфраструктурни пружаоци платних услуга – SWIFT, картичне шеме и сл.) и пружаоцима ИКТ услуга, укључујући и ризике који произилазе из ланаца снабдијевања, - редовно скенирање рањивости, периодично пенетрационо тестирање и праћење сајбер пријетњи (*threat intelligence*, CERT обавјештења и др.), - редовно преиспитивање, ажурирање и тестирање сценарија ризика (нпр. ransomware напад на критични систем, дуготрајни прекид рада интернет провајдера, компромитација података код пружаоца ИКТ услуга, отказ кључне инфраструктуре,…), те извјештавање Управе банке.
Подручје	**Управљање ИКТ ризицима**
Датум одговора	10.02.2026.
Тема	**План примјене мјера** (члан 16. став 4)
	(4) Банка је дужна усвојити план примјене мјера и континуирано

	пратити реализацију овог плана. Овај план најмање укључује преглед свих идентификованих ризика, опис корективних мјера, приоритете и рокове за провођење, одговорна лица. Уколико банка пролонгира рок за неприхватљиве ризике дужна је о томе благовремено обавијестити Агенцију.
Питање банке бр. 15	Дефиниција појма неприхватљиви ризици
Одговор Агенције	У складу са чланом 14. став 2. Одлуке, Банка је дужна да утврди ниво толеранције на ИКТ ризик у складу са својим склоношћу (апетитом) за преузимање ризика. Утврђивање нивоа толеранције на ИКТ ризик подразумијева и дефинисање ризика који се сматрају неприхватљивим, као и утврђивање мјере контроле и ублажавања које ће бити примјењене када ризик премаши утврђене границе толеранције или може довести до значајних финансијских губитака, нарушавања континуитета пословања, регулаторних санкција или озбиљног утицаја на репутацију банке.
Подручје	**Одговорности и управљање ИКТ ризицима**
Датум одговора	10.02.2026.
Тема	**Политика информационе безбједности** (члан 6. и 17. став 4. тачка 1)
	(2) Лице из става 1. овог члана треба да надзире и координише активности у вези са информационом безбједношћу, а што укључује најмање сљедеће: *...4) учествује у изради политике информационе безбједности, из члана 17. ове одлуке, те даје приједлоге за њено унапређење, у складу са развојем ИКТ система и ИКТ ризика у банци,* *(4) У склопу оквира за управљање ИКТ ризицима, банка је дужна:* *1) да усвоји и имплементира политику информационе безбједности, којом се дефинишу правила за заштиту доступности, аутентичности, интегритета и повјерљивости података, те информационе и ИКТ имовине, како би се постигли циљеви у области информационе безбједности,*
Питање банке бр. 16	Ко је овлаштен да креира политику информационе безбједности прописану наведеним чланом? Да ли је то одговорно лице за безбједност информационог система?
Одговор Агенције	Члан 17. став 4. тачка 1) Одлуке прописује обавезу банке да усвоји и имплементира политику информационе безбједности у циљу заштите доступности, аутентичности, интегритета и повјерљивости података, као и информационе и ИКТ имовине. Агенција истиче да, иако одговорно лице за безбједност информационог система (CISO) има кључну улогу у припреми и приједлогу политике, коначна одговорност за усвајање и имплементацију политике информационе безбједности лежи на **Управи банке** и **Надзорном одбору**. Одговорно лице за безбједност информационог система има задатак да: - иницира израду политике,

	- обезбиједи да политика буде у складу са регулаторним и интерним захтјевима, - координише консултације са релевантним функцијама у банци, - прати примјену и ревизију политике. На овај начин се осигурава да политика има формални ауторитет у банци и да је примјена њених одредби ефикасна у свим ИКТ процесима.
Подручје	**Управљање ИКТ ризицима**
Датум одговора	10.02.2026.
Тема	**Сегрегација дужности** (члан 18. став 3.)
	(3) Банка је дужна осигурати адекватну сегрегацију дужности запослених у процесу надзора и процесима који су предмет надзора.
Питање банке бр. 17	Молимо за детаљније појашњење или примјер сегрегације дужности запослених у процесу надзора и процесима који су предмет надзора из члана 18. став 3. Одлуке, те да ли је сегрегацију потребно направити унутар ИТ сектора?
Одговор Агенције	Сегрегацију дужности није неопходно у свим случајевима успостављати унутар ИТ сектора. Она је потребна уколико су у оквиру ИТ сектора обједињене извршне и надзорне/контролне активности над истим ИКТ процесима или системима. У случајевима када су надзорне функције организационо издвојене из ИТ сектора, захтјев сегрегације је испуњен на нивоу банке. Сегрегација јесте потребна унутар ИТ сектора ако: - информациона безбједност, - управљање рањивостима, - SIEM / логовање, - одобравање промјена, - контрола приступа организационо припадају ИТ-у и представљају прву линију одбране. Тада се мора показати да: - исти запослени не извршава и не надзире исти процес, - постоје јасне улоге, принцип „четири ока“ или независна верификација.
Подручје	**Управљање ИКТ ризицима повезаним са трећим странама**
Датум одговора	10.02.2026.
Тема	**Уговори о употреби ИКТ услуга** (члан 24. став 1. тачка 2)
	(1) Прије склапања уговора о употреби ИКТ услуга банка је дужна: ....2) процијенити да ли су испуњени регулаторни захтјеви у погледу уговарања
Питање банке бр. 18	Појашњење регулаторних захтјева
Одговор Агенције	Под појмом „регулаторни захтјеви у погледу уговарања“ (став 1. тачка 2.) подразумијевају се све одредбе прописане одлукама и упутствима Агенције, с посебним освртом на могућност ефикасног надзора пружања услуга од стране Агенције, банке и од њих овлаштених страна, укључујући: - могућност надзора на мјесту обављања услуге,

	- правовремени приступ подацима и системима који су предмет надзора, - осигурање да надзор буде изводљив и ефикасан у складу са важећим регулаторним оквиром.
Подручје	**Управљање ИКТ ризицима повезаним са трећим странама**
Датум одговора	10.02.2026.
Тема	**Уговор о употреби ИКТ услуга** (члан 24. став 1. тачка 4)
	(1) Прије склапања уговора о употреби ИКТ услуга банка је дужна: …4) проводити дубинске анализе потенцијалних пружаоца ИКТ услуга и обезбиједити прикладност пружаоца ИКТ услуга током цијелог процеса избора и процеса процјене
Питање банке бр. 19	Да ли је провођење дубинске анализе обавезно за све пружаоце ИКТ услуга (укључујући и екстернализоване)? Да ли је потребно мијењати и Одлуку о управљању екстернализацијом? Шта се подразумијева под „обезбиједити прикладност пружаоца ИКТ услуга“?
Одговор Агенције	Независно од одредби Одлуке о управљању екстернализацијом, банка је дужна управљати ИКТ ризицима повезаним са трећим странама, као саставним дијелом оквира за управљање ИКТ ризицима из члана 12. ове одлуке. Дефинисано је да је Пружалац ИКТ услуга је трећа страна која обавља одређену активност из подручја ИКТа, дјелимично или у цјелини, на основу уговора закљученог са банком. Прикладност пружаоца ИКТ услуга подразумијева се да банка, прије закључења уговора и током цијелог трајања уговорног односа, утврди и документује да је пружалац ИКТ услуга: 1. организационо, технички и кадровски способан да пружа уговорене ИКТ услуге на начин који не угрожава дигиталну оперативну отпорност банке, 2. усклађен са релевантним регулаторним захтјевима, укључујући захтјеве у области информационе безбједности, заштите података, управљања ИКТ ризицима и екстернализације, 3. у могућности да обезбиједи континуитет, доступност, интегритет, аутентичност и повјерљивост података и ИКТ система који подржавају пословање банке, 4. располаже одговарајућим политикама, процедурама и контролама, укључујући управљање инцидентима, управљање промјенама, резервне копије, опоравак од катастрофе и тестирање, 5. има стабилан финансијски и оперативни профил, који не представља повећан ризик за прекид или деградацију пружања ИКТ услуга, 6. омогућава банци и надзорном органу приступ, надзор и ревизију, у складу са регулаторним захтјевима, 7. има јасно дефинисане ланце подуговарања, уз контролу ризика који произилазе из подизвођача, посебно уколико се ради о услугама које подржавају критичне функције или кључне пословне активности.

Подручје	**Управљање ИКТ ризицима повезаним са трећим странама**
Датум одговора	10.02.2026.
Тема	**Уговор о употреби ИКТ услуга** (члан 24. став 2.)
	(2) Банка је дужна склапати уговоре искључиво са пружаоцима ИКТ услуга који примјењују одговарајуће стандарде ИКТ безбједности. Уколико се уговор односи на услуге које подржавају критичне функције или кључне пословне активности, банка је дужна, прије склапања уговора утврдити да пружалац услуга примјењује релевантне и признате стандарде ИКТ безбједности.
Питање банке бр. 20	Потребно је да се детаљније појасне и дефинишу стандарди ИКТ безбједности које су дужни да примјењују пружаоци услуга са којима банка склапа уговоре.
Одговор Агенције	У складу са чланом 24. став 2. Одлуке банка је дужна да склапа уговоре искључиво са пружаоцима ИКТ услуга који примјењују одговарајуће стандарде ИКТ безбједности, при чему се посебан фокус ставља на услуге које подржавају критичне функције или кључне пословне активности. Под „одговарајућим“ и „релевантним и признатим“ стандардима ИКТ безбједности подразумијевају се стандарди и праксе које су опште прихваћене у ИКТ и које обезбјеђују адекватан ниво безбједности у складу са циљевима банке и регулаторним захтјевима (нпр. ISO/IEC 27001 , ISO/IEC 27002, ISO/IEC 22301, ISO/IEC 27701, ISO/IEC 27017 и ISO/IEC 27018, PCI DSS, други еквивалентни стандарди или независне процјене које пружају упоредив ниво сигурности) Банка је дужна прије склапања уговора утврдити да пружалац ИКТ услуга примјењује ове или еквивалентне стандарде који обезбјеђују сигурност услуге у складу са регулаторним и интерним безбједносним циљевима. Обавеза праћења и редовне провјере усклађености са стандардима регулисана је чланом 24. ставом 3. Одлуке.
Подручје	**Управљање ИКТ ризицима повезаним са трећим странама**
Датум одговора	10.02.2026.
Тема	**Обавеза усклађивања уговора о употреби ИКТ услуга** (члан 24. и 27.)
Питање банке бр. 21	Да ли постоји обавеза усклађивања постојећих уговора о употреби ИКТ услуга или се одредбе Одлуке односе само на нове уговоре?
Одговор Агенције	Обавеза усклађивања односи се и на постојеће и на нове уговоре о употреби ИКТ услуга. Банка је дужна да постојеће уговоре усклади са одредбама Одлуке до почетка њене примјене, а најкасније у оквиру редовне годишње процјене пружаоца ИКТ услуга.
Подручје	**Управљање ИКТ ризицима**
Датум одговора	10.02.2026.
Тема	**Уговор о употреби ИКТ услуга** (члан 27. став 3. тачка 4.)
	(3) Уговори о употреби ИКТ услуга, поред услова из става 2. овог члана, требају укључити и сљедеће: *...4) услове за учествовање пружаоца ИКТ услуга у програмима за*

	подизање свијести о безбједности у подручју ИКТ-а и оспособљавањима о дигиталној оперативној отпорности које проводи банка, а у складу са чланом 21. ове одлуке,
Питање банке бр. 22	Да ли се члан 27. став 3. тачка 4. може тумачити тако да Банка треба да у своје програме за подизање свијести укључи и пружаоце ИКТ услуга?
Одговор Агенције	Да, на начин да уговори о употреби ИКТ услуга треба да омогуће и уреде учешће пружаоца ИКТ услуга у релевантним активностима подизања свијести и оспособљавања, у мјери у којој је то оправдано природом и значајем услуге коју пружа, као и процјеном ризика. У том смислу, учешће пружаоца ИКТ услуга може бити ограничено на циљане активности, размјену релевантних информација, или прилагођене облике сарадње, а не нужно на пуно укључивање у интерне програме банке. Обим и начин таквог учешћа дефинишу се уговором, уз примјену принципа пропорционалности.
Подручје	**Управљање ИКТ ризицима повезаним са трећим странама**
Датум одговора	10.02.2026.
Тема	**Уговори о употреби ИКТ услуга** (члан 27. став 4. тачка 4. подтачка 2)
	(4) Уговори о употреби ИКТ услуга које подржавају критичне функције и кључне пословне активности, требају бити усаглашени са чланом 9. ставом 4. Одлуке о управљању екстернализацијом и ставом 3. овог члана, а укључују и сљедеће: *...4) право на континуирано праћење рада пружаоца ИКТ услуге, што укључује следеће:* *....2. право уговарања алтернативних нивоа осигурања ако су обухваћена права других клијената*
Питање банке бр. 23	Која врста осигурања је потребна? Шта се мисли под правима других клијената?
Одговор Агенције	Право уговарања алтернативних нивоа осигурања односи се на могућност прилагођавања уговорних услова са пружаоцима ИКТ услуга који пружају ИКТ услуге за више клијената, под условом да таква прилагођавања не утичу негативно на права и уговорне обавезе према другим клијентима тог пружаоца услуга.
Подручје	**Управљање ИКТ ризицима повезаним са трећим странама**
Датум одговора	10.02.2026.
Тема	**Излазне стратегије** (члан 27. став 4. тачка 5.)
	(4) Уговори о употреби ИКТ услуга које подржавају критичне функције и кључне пословне активности, требају бити усаглашени са чланом 9. ставом 4. Одлуке о управљању екстернализацијом и ставом 3. овог члана, а укључују и сљедеће: *...5) излазне стратегије, посебно дефинисање обавезног прелазног периода:* *1. током којег ће пружалац ИКТ услуга наставити пружати предметне активности или ИКТ услуге банци како би се смањио ризик од поремећаја у раду банке или како би се осигурао њен ефикасан опоравак и реструктурирање и*

	2. у којем банка може изабрати другог пружаоца ИКТ услуга или враћање предметне активности у банку, у складу са сложеношћу услуге која је предмет уговора.
Питање банке бр. 24	Да ли Банка наведено треба да усагласи и кроз уговор са пружаоцем услуге и да ли се наведени захтјев односи и на пружаоце материјалних и активности које нису материјално значајне?
Одговор Агенције	Банка наведени захтјев примарно имплементира кроз одговарајуће уговорне одредбе са свим пружаоцима ИКТ услуга, у мјери у којој је то примјењиво и пропорционално сложености и значају услуге која је предмет уговора. Уговори о употреби ИКТ услуга које подржавају критичне функције и кључне пословне активности, требају бити усаглашени са чланом 9. ставом 4. Одлуке о управљању екстернализацијом и ставом 3. овог члана. Уговорно уређивање прелазног периода представља један од механизама за обезбјеђивање ефикасне примјене излазне стратегије, али не искључује и друге интерне или оперативне мјере које банка може примјењивати.
Подручје	**Управљање ИКТ операцијама**
Датум одговора	10.02.2026.
Тема	**Регистар ИКТ система** (члан 30. став 7.)
	(7) У складу са процјеном ризика, банка је дужна примјењивати поступке набавке и развоја ИКТ система и на оне ИКТ системе које развијају или којима управљају крајњи корисници у пословним функцијама изван ИКТ организације. Банка је дужна водити регистар оваквих система који су подршка критичним пословним функцијама или процесима.
Питање банке бр. 25	Молимо за појашњење/примјер ИКТ система које развијају или којима управљају крајњи корисници у пословним фунцкијама изван ИКТ организације из члана 30. став 7. Одлуке?
Одговор Агенције	Под ИКТ системима које развијају или којима управљају крајњи корисници у пословним функцијама изван ИКТ организације, у смислу члана 30. став 7. Одлуке, подразумијевају се рјешења која настају у оквиру пословних организационих јединица ради подршке конкретним пословним процесима, а која нису развијена, имплементирана или оперативно управљана од стране ИКТ организације банке. Овакви системи у пракси могу обухватати, између осталог: - табеларне и базе података креиране од стране пословних корисника (нпр. сложени Excel/Access фајлови), - локалне или *cloud*-базиране апликације развијене коришћењем *low-code/no-code* платформи, - скрипте, алате и аутоматизације креиране од стране корисника ради обраде, извјештавања или контроле података, - апликације или алате које пословне функције самостално набављају, одржавају или конфигуришу, без формалног укључивања ИКТ организације. Одредба члана 30. став 7. има за циљ да обезбиједи да и овакви системи, уколико подржавају критичне пословне функције или

	процесе, буду идентификовани, евидентирани у одговарајућем регистру и обухваћени пропорционалним мјерама управљања ризиком, без обзира на то што су настали изван формалног ИКТ развојног тима.
Подручје	**Управљање ИКТ инцидентима**
Датум одговора	10.02.2026.
Тема	**Показатељи за рано упозорење инцидента** (члан 32. став 2. тачка 1.)
	(2) Банка је дужна у оквиру процеса управљања ИКТ инцидентима из става 1. овог члана: *1) успоставити показатеље за рано упозорење,*
Питање банке бр. 26	Молимо за појашњење члана 32. став 2. тачка 1. Одлуке, на шта/које показатеље раног упозорења се конкретно мисли? Чланом 32. став 2. Одлуке прописано је да је Банка дужна у оквиру процеса управљања ИКТ инцидентима, између осталог, успоставити показатеље за рано упозорење. Да ли се ради о одређеном мониторингу?
Одговор Агенције	Банка треба успоставити алате за праћење ИКТ система у реалном времену, дефинисати прагове (thresholds) за алармирање, те прикупљати и анализирати податке о актуелним пријетњама.
Подручје	**Тестирање дигиталне оперативне отпорности**
Датум одговора	10.02.2026.
Тема	**Провођење тестова** (члан 35. став 5. тачка 1.)
	(5) Банка је дужна обезбиједити да се одговарајући тестови редовно проводе, поштујући сљедеће: *1) најмање једном годишње за све ИКТ системе и апликације који подржавају критичне функције и кључне пословне активности,*
Питање банке бр. 27	Да ли се члан 35. став 5. тачка 1. може тумачити да се сви тестови наведени у члану 36. морају спроводити једном годишње?
Одговор Агенције	Одредба члана 35. став 5. тачка 1) Одлуке прописује обавезу да се за ИКТ системе и апликације који подржавају критичне функције и кључне пословне активности редовно спроводе одговарајући тестови, најмање једном годишње, у циљу очувања дигиталне оперативне отпорности банке. У том контексту, тестирање дигиталне отпорности из члана 36. представља оквир релевантних врста тестирања које банка треба да примјењује над наведеним ИКТ системима и апликацијама, у складу са њиховом критичношћу, сложеношћу и изложеношћу ризицима. Сходно наведеном, за ИКТ системе и апликације који подржавају критичне функције и кључне пословне активности, очекује се да програм тестирања обухвати све релевантне врсте тестова наведене у члану 36., те да се исти проводе најмање једном годишње, уз могућност да банка, на основу процјене ризика, одреди динамику и обим појединих тестова у оквиру наведеног минималног захтјева.
Подручје	**Тестирање дигиталне оперативне отпорности**
Датум одговора	10.02.2026.
Тема	**Провођење тестова** (члан 38. став 2.)

	(2) Агенција ће утврдити које банке су дужне проводити TLPT, узимајући у обзир принцип пропорционалности, а имајући у виду сљедеће: *1) факторе које утичу на финансијски сектор, с посебним освртом на степен у којем услуге и активности које банка пружа утичу на финансијски сектор у цјелини,* *2) потенцијални утицај на стабилност финансијског сектора, укључујући системски значај банке,* *3) специфични ИКТ профил ризика, ниво ИКТ зрелости банке или карактеристика коришћених технологија.*
Питање банке бр. 28	Када се очекује да ће Агенција утврдити које су банке дужне спроводити TLPT сходно наведеном члану Одлуке?
Одговор Агенције	Агенција ће благовремено, а најмање 12 мјесеци прије обавезе провођења ових тестирања обавијестити банке које су дужне проводити TLPT.
Подручје	**Управљање континуитетом пословања**
Датум одговора	10.02.2026.
Тема	**Резервне копије података** (члан 47. став 3.)
	(3) ИКТ системи који се користе за обнављање и опоравак података, морају бити физички и логички одвојени од изворних ИКТ система, те заштићени од неовлашћеног приступа или оштећења у подручју ИКТ система.
Питање банке бр. 29	Да ли одредба члана 47. став 3. у пракси значи да се системи за креирање резервних копија не могу налазити у примарном дата центру гдје се налазе и изворни ИКТ системи?
Одговор Агенције	Системи за креирање резервних копија се могу налазити у примарном дата центру гдје се налазе и изворни ИКТ системи, али морају бити физички и логички одвојени од ових система. Захтјев за физичком и логичком одвојеношћу подразумијева да су системи за обнављање и опоравак података пројектовани и имплементирани на начин који обезбјеђује њихову независност од изворних ИКТ система, те отпорност на заједничке тачке отказа, неовлашћени приступ и компромитацију података. Такође, ставом 4. овог члана, дефинисано је да је Банка дужна обезбиједити да се резервне копије података чувају на једној или више секундарних локација, од којих најмање једна мора бити довољно удаљена од примарне локације, на којој се налазе изворни подаци, тако да нису изложене истим ризицима. Банка примјењује принцип процјене ризика и пропорционалности при дефинисању архитектуре система за резервне копије, узимајући у обзир критичност података и функција, те обезбјеђује додатне локацијске или техничке мјере у случајевима гдје је то оправдано ради постизања одговарајућег нивоа оперативне отпорности.